

UNITED STATES DISTRICT COURT

for the
Eastern District of Missouri

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)THE PREMISES LOCATED AT: 11830 Claremont, Wright City,
MO, 63390

)}

Case No. 4:20 MJ 95 DDN

SIGNED AND SUBMITTED TO THE COURT

FOR FILING BY RELIABLE ELECTRONIC MEANS

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

located in the EASTERN District of MISSOURI, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

evidence of a crime;
 contraband, fruits of crime, or other items illegally possessed;
 property designed for use, intended for use, or used in committing a crime;
 a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

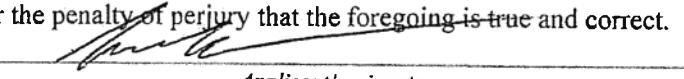
<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. Section 2252A(a)(2)	Receipt of Child Pornography
18 U.S.C. Section 2252A(a)(5)(B)	Possession of Child Pornography

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

Continued on the attached sheet.
 Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the foregoing is true and correct.


Applicant's signature

David Rapp, Special Agent, FBI

Printed name and title

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41.

Date: April 10, 2020

/s/ David D. Noce

Judge's signature

David D. Noce, U.S. Magistrate Judge

Printed name and title

City and state: St. Louis, MO

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF) No. 4:20 MJ 95 DDN
THE PREMISES LOCATED AT: 11830)
Claremont, Wright City, MO, 63390) SIGNED AND SUBMITTED TO THE
) COURT FOR FILING BY RELIABLE
) ELECTRONIC MEANS
)
) **FILED UNDER SEAL**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, David Rapp, a Special Agent (SA) with the Federal Bureau of Investigation (FBI), St. Louis Division, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises located at 11830 Claremont Lane, Wright City, MO, 63390, (hereinafter the "SUBJECT PREMISES"), further described in Attachment A, for the things described in Attachment B.

2. I have been employed as a Special Agent of the FBI since 2001, and I am currently assigned to the FBI St. Louis Division. While employed by the FBI, I have investigated federal criminal violations related to matters involving the online sexual exploitation of children. I have gained experience through training at the FBI Academy, post academy training, and everyday work related to conducting these types of investigations.

3. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended

to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 2252A(a)(2) (Receipt of Child Pornography) and 2252A(a)(5)(B) (Possession of Child Pornography) (hereafter referred to as the “TARGET OFFENSES”) have been committed by **Phillip Michael Parmley**, or other persons known and unknown. There is also probable cause to search the residence described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

DEFINITIONS

6. The following terms have the indicated meaning in this affidavit:

a. The term “minor” means any individual under the age of 18 years. 18 U.S.C. § 2256(1).

b. Sexually explicit conduct means actual or simulated sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the anus, genitals, or pubic area of any person. 18 U.S.C. § 2256(2)(A).

c. Visual depiction includes undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image. 18 U.S.C. § 2256(5).

d. Child pornography means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct or such visual

depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct. 18 U.S.C. § 2256(8)(A) or (C).

e. Identifiable minor means a person who was a minor at the time the visual depiction was created, adapted, or modified; or whose image as a minor was used in creating, adapting, or modifying the visual depiction; and who is recognizable as an actual person by the person's face, likeness, or other distinguishing characteristic, such as a unique birthmark or other recognizable feature; and shall not be construed to require proof of the actual identity of the identifiable minor. 18 U.S.C. § 2256(9).

f. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means.

g. Electronic data may be more fully described as any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer-related equipment.

h. "Wireless telephone or mobile telephone, or cellular telephone or cell phone or smartphone" as used herein means is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet.

Wireless telephones may have wireless connection capabilities such as Wi-Fi and Bluetooth. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

LOCATION TO BE SEARCHED

7. The location to be searched is: 11830 Claremont, Wright City, MO, 63390, and is identified as follows: The residence is a single family home, with a detached garage, that is brown in color with tan brick, and is a 3 bedroom, 2.5 bath, approximate 2,500 square foot in size and on an approximate 3 acre lot. The residence is listed on Accurint as being owned by Ronald Parmley and Sandra Boyd.

8. The SUBJECT PREMISES include, but is not limited to: a large, approximate 16 feet in length PODS container located on the driveway, and any vehicles located on the premises and under the control of **Phillip Michael Parmley**, to include, a 2010 Kia Rio, Missouri License Plate CV1A1G.

PROBABLE CAUSE

9. In August of 2018, an investigation out of the FBI Birmingham Division identified an online user, David Aaron Drake, in the Birmingham AOR who utilized TUMBLR to advertise, sell, and distribute child pornography.

10. Drake would share other users’ postings of child pornography to his own TUMBLR blog and would refer the users to his WICKR account to buy links. Drake would post things like, “Wickr sendmb6 to buy links,” on each of the photos of child pornography Drake shared to his own TUMBLR blog. Once Drake was contacted on WICKR, Drake would share a screenshot of multiple folders from his MEGA account. The folders were divided up by genre (man versus boy, boy on boy, etc...) of child porn and acted as a “menu” for the purchasers. The folders mainly contained videos of child pornography. Each folder was priced based on the quantity and quality

of child pornography contained within. Folder prices ranged from \$10 to \$50.

11. Once the purchaser selected a folder to purchase, Drake offered three (3) forms of payment: VENMO, CASH APP and AMAZON gift cards. Once a purchase was complete, Drake would send a link to the specific folder purchased and the user could download contents of the folder. Drake utilized AMAZON gift cards for international purchasers who did not have access to VENMO or CASH APP.

12. In September 2018, Agents with the FBI Birmingham Division conducted three (3) controlled buys of child pornography from Drake. The first purchase resulted in a folder that was priced at \$40. Agents received access to the folder which contained 640 videos of child pornography. The second purchase resulted in access to an online private chat group, whom openly shared child pornography, in the TELEGRAM app. The third controlled purchased resulted in access to one of Drake's DROPBOX accounts, which resulted in access to hundreds of images and videos of child pornography.

13. In October 2018, a federal search warrant was executed on the apartment of Drake by Agents with the FBI Birmingham Division which ultimately resulted in the arrest of Drake. Drake signed consent for Agents of the FBI Birmingham Division to assume all online identities.

14. In May 2019, Drake plead guilty to a five (5) count federal indictment (Advertisement - 2 counts; Sale; Possession - 2 counts) and offered to proffer on the information. Drake stated he solely used his VENMO, CASH APP and the specific AMAZON account for the sale and distribution of child pornography. Drake instructed users to say the payments were for tutoring, books or other college related expenses to throw off law enforcement authorities.

15. Administrative subpoenas were sent by Agents from the FBI Birmingham Division to VENMO, CASH APP and AMAZON regarding Drake's accounts. Several users who purchased from Drake were identified utilizing records from VENMO, CASH APP and AMAZON. These

records were compared to records on ACCURINT and used to identify purchasers around the country. According to CASH APP records user, “Christ” completed the following transactions to DRAKE:

- 08/23/2018 at 2:18 PM, “Christ” completed a transaction for \$30. The details of the transaction were listed as “eheh.”
- 08/24/2018 at 1:35 AM, “Christ” completed a transaction for \$30. The details of the transaction were listed as “huh.”
- 08/26/2018 at 27:26 AM, “Christ” completed a transaction for \$30. The details of the transaction were listed as “hd.”
- 09/15/2018 at 12:29 AM, “Christ” completed a transaction for \$30. The details of the transaction were listed as “NA.”
- 09/16/2018 at 7:30 PM, “Christ” completed a transaction for \$30. The details of the transaction were listed as “link.”
- 09/19/2018 at 4:19 AM, “Christ” completed a transaction for \$30. The details of the transaction were listed as “link.”
- 09/23/2018 at 11:59 PM, “Christ” completed a transaction for \$40. The details of the transaction were listed as “link.”

16. An administrative subpoena sent by Agents from the FBI Birmingham Division to CASH APP regarding user “Christ” revealed the following information: Customer Token: C_fapmj8yaz, Name: CHRIST CHRISTIAN HOCK, date of birth 03/17/1992, last four of social security number 8166, telephone number 3146657170, residing at 4053 Broad St, Saint Charles, MO 63301.

17. An ACCURINT search for Christian Hock, date of birth: XX/XX/1992, conducted by Agents from the FBI Birmingham Division, revealed the following information: Name: Christian John Hock. Address: 5522 Delmar Blvd., Apt 204, St. Louis, MO 63112-3050, SSN: XXX-XX-8166.

18. On February 11, 2020, your affiant and Task Force Officer (TFO) Michael Spreck contacted Hock at 5522 Delmar Boulevard, Apartment 204, St. Louis, MO. After advising Hock of the investigator's identities and the nature of the interview, HOCK agreed to speak with your affiant and TFO Spreck.

19. Hock was advised of his *Miranda* Rights on audio recording and was advised that he was being recorded. Hock acknowledged his *Miranda* Rights and agreed to speak with the investigators. At that time, Hock admitted to purchasing child pornography on multiple occasions during the time frame of August and September of 2018. Hock advised that he used his Samsung Galaxy S9 cellular telephone to download the aforementioned files and to pay for them via Cash App. Hock advised that he was still in possession of this Samsung Galaxy S9 cellular telephone and provided his consent via signed form to allow investigators to take this phone and to search it. Hock believed that he currently only had 5 to ten pictures of child pornography on this Samsung S9 cellular telephone and that he did not believe any of them to still be from those that he bought in August and September of 2018.

20. On February 21, 2020, a search warrant was applied for by your affiant and authorized within the Eastern District of Missouri for Hock's seized cellular telephone (4:20-MJ-3093 NCC). This search warrant was executed on the same date by your affiant and analysis was conducted on Hock's cellular telephone by technically trained FBI Agents in the St. Louis Division.

21. Through analysis by your affiant found multiple images and videos of child pornography that were located on Hock's cellular telephone.

22. It was also determined by your affiant that Hock had shared child pornographic images via a social media application called Telegram. Specifically, Hock sent videos and

photographs containing child pornography to Telegram user “Philip.” The Telegram profile for “Philip” listed telephone number (636) 385-3509 as the contact number.

23. Your affiant reviewed Telegram’s website, specifically <https://telegram.org/faq#q-which-devices-can-i-use>, which states that Telegram is a free messaging application launched in 2013, that is currently located in Dubai, UAE. Telegram users can utilize the application across all devices at the same time and messages are synced seamlessly across any number of user owned phones, tablets or computers.

24. The Telegram website states that a Telegram account is connected to a cellular phone number, and that users receive a verification code at that phone number to use the application on a particular device. The website further states that the application can be used on both the IOS and Android based cellular phone and tablet systems, as well as via a desktop application for Windows, macOS, and Linux computer operating systems. Further the website states that a user can log into Telegram from as many user owned devices as available, all at the same time and that the user just needs to use their main telephone number to log in from any device.

25. Telegram advises that all Telegram chats and group chats are private amongst participants and that they do not process any legal requests related to user activity. The user chats are end to end encryption and as such they do not have any data to disclose. To date, Telegram advises that they have disclosed 0 bytes of user data to third parties, including governments.

26. Your affiant reviewed messages between Hock and “Philip” within the Telegram application installed on Hock’s cellular device, including the following:

a. On December 2, 2019, Hock sent a message to “Philip” stating “Fuck even use a dildo on a boy.” In response, “Philip” replied “Yum.” Hock then replied “Open up that tiny, light pink hole.” “Philip” replied “Heh. i need a daddy cock to help me.” Hock replied “Mmmm.

Shoot loads of cum in him.” “Philip” replied “Yessir, holy hell i just shot a huge load.” Later in the message conversation, Hock sent a message “I’d eat the cum out of a boys ass.” “Philip” replied “Lol that would be hot.”

b. On December 14, 2019, Hock asks “Philip” if he is still in contact with the “guys” that have a kid and animals in Wentzville. There is no record of “Philip” providing any response to this question. However, it should be noted that an FBI St. Louis Division analyst conducted an open source search using the term, “Phillip Parmley.” The results revealed Facebook account: FB ID 1297050157, vanity name phillip.parmley, profile name Phillip Parmley. Phillip Parmley is Facebook friends with Sara Brenneman who resides in Wentzville, Missouri, and has a son that appears to be under the age of eight. Brenneman’s Facebook states that she is in a relationship with Matt Bauer.

c. On December 22, 2019, “Philip” asks Hock “Whatchu up to.” Hock replies “Watching TV but not watching TV lol getting distracted by my horniness haha. Thinking about horse cock and young boys.” “Philip” replies “Lol nice. I’m watching vYouTube, been wanting to see some cp lately.” Hock then sends “Philip” a photograph entitled “OkshTYwk.jpg”. This photograph depicts a toddler aged boy being anally penetrated by an adult penis. “Philip” replies “Yum. What kind of longer vids you have, wickr has a pretty short limit doesn’t it? Lol.” Hock then sends “Philip” a video entitled “M3.mp4.” This video depicts a toddler aged child being annually penetrated with a penis by an adult male. In a text exchange following the video being sent “Philip” advises “That’s a bit much for me.” Hock replies “It’s a super famous one. It scared me the first time I watched it.” “Philip” replies “Yeah, I prefer willingness, crying and pain, that’s just sheer torture.”

d. On December 22, 2019, Hock also sends “Philip” a photo entitled “photo-1206041.png.” This image depicts three naked men engaging in sexual activity with farm animals,

possibly small calves. Hock replies “Yeah I’m the same. One reason why I like 5/6+.” “Philip” replies “Same. That’s a hot pic.”

e. On December 22, 2019, Hock then sends “Philip” a video entitled “75438fc144.360.mp4”. This video depicts an adult male inserting his penis into the rectum of a young, pre-teen aged boy in various sexual positions. The adult male then ejaculates onto the penis of the boy. “Philip” replies to Hock “Fuck that one is hot af. Came already.”

f. On January 14, 2020, Hock sends a message to “Philip” stating “Perved out lately?” “Philip” replied “Nah, been erasing my accounts, forgot i didn’t delete this one yet. Going to start a YouTube channel. Want to eliminate all potential hazards.” “Philip” then advised Hock that he had won a \$400 Go Pro Hero 7 camera at work and that he “might as well use it.”

27. A subpoena sent to AT&T revealed that telephone number (636) 385-3509 is subscribed to **Phillip Parmley**, at the SUBJECT PREMISES with email address pparmley384@gmail.com. As of the date of this affidavit, this phone number was still active and showed a service start date of July 24, 2019.

28. On April 5, 2020, at approximately 1:00 pm, your affiant traveled to the SUBJECT PREMISES. At that time, your affiant observed a brownish-red, Kia Rio, MO License Plate CV1A1G parked near the driveway in front of the SUBJECT PREMISES. A Missouri Department of Revenue check reveals that this vehicle has a current and valid registration and is registered to **Phillip M. Parmley** and Danielle Gagliani, with an address of the SUBJECT PREMISES. In addition, your affiant observed a large, approximate 16 feet in length, white PODS container located on the driveway of the SUBJECT PREMISES.

29. On April 6 and 7, 2020, at approximately 4:30 pm, St Charles County Police Department (SCCPD) Violent Crimes Against Children (VCAC) Task Force Officer (TFO) Andrew Sitton traveled to the SUBJECT PREMISES. At that time, TFO Sitton observed the

aforementioned brownish-red, Kia Rio, MO License Plate CV1A1G parked on the street in front of the SUBJECT PREMISES. In addition, TFO Sitton also observed the large PODS container located on the driveway of the SUBJECT PREMISES, and was able to see that the container was filled with household items.

30. On April 8, 2020, at approximately 7:20 am, TFO Andrew Sitton traveled to the SUBJECT PREMISES. At that time, TFO Sitton observed the aforementioned brownish-red, Kia Rio, MO License Plate CV1A1G parked on the street in front of the SUBJECT PREMISES. In addition, TFO Sitton also observed the PODS container located on the driveway of the SUBJECT PREMISES.

31. On April 8, 2020, your affiant visited the Zillow.com website related to the SUBJECT PREMISES and noticed that the SUBJECT PREMISES is listed for sale by owner, and was listed for sale on February 11, 2020.

32. An Accurint check conducted by your affiant revealed that the SUBJECT PREMISES¹ is the current address for **Phillip M. Parmley** since July of 2013.² In addition, according to the Missouri Division of Employment Security, which is an agency that records the amounts of income paid to and income taxes paid by individuals who are employed or reside in Missouri, the listed address for **Philip M. Parmley** is the SUBJECT PREMISES.

I. CHARACTERISTICS OF PORNOGRAPHY PARTICIPANTS

33. In addition to participating in child exploitation investigations, your affiant has discussed the aspects of computers and their relationship with child pornography offenses with

¹ It should be noted that various mapping programs and database websites refer to “Claremont Lane” and “Claremont Avenue.” Your affiant has confirmed that there is only one street named “Claremont” in Wright City, Mo.

² It should be noted that Accurint also lists 41 Rocky Brook Court, Lake St. Louis, MO as a potential address for Philip Michael Parmley. However, to date, Parmley’s vehicle has only been observed at the SUBJECT PREMISES.

others. Based upon my knowledge, experience, and communications with other individuals involved in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt and collection of child pornography.

34. Based on my training and experience, and the training and experience of other agents, I believe that a resident residing at the SUBJECT PREMISES is a collector of child pornography and/or possibly a producer of child pornography. I base this conclusion on the following facts:

a. Individuals who receive and collect child pornography may receive sexual gratification, stimulation, and satisfaction viewing children engaged in sexual activity, in sexually suggestive poses such as in person, in photographs, other visual media, or from literature describing such activity. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Based on the evidence obtained in this investigation, **Phillip Michael Parmley** viewed child pornography sent to him by Hock and did not protest and even commented as to liking at least one video when he advised “Fuck that one is hot af.”

b. Individuals who receive and collect child pornography do so in a variety of media, including, but not limited to, digital images and videos of child pornography. Based on the evidence obtained in this investigation, **Phillip Michael Parmley** utilized the Telegram Application to view and collect videos of child pornography, which can be accessed via multiple forms of electronic devices, including cellular telephones, tablets and computers.

c. Individuals who receive and collect child pornography almost always possess and maintain their “hard copies” of child pornographic material, that is, their pictures, films, videotapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location.

Maintaining these collections in a digital or electronic format in a safe, secure and private environment, such as a computer in a private residence, allows the collectors the opportunity to safely maintain their collections for many years and enable the collector to frequently view the collection, which is valued highly. Based on the evidence obtained in this investigation, files of child pornography are likely being stored on electronic devices at this private residence.

d. Child pornography collectors may also correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit materials; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. Based on the evidence obtained in this investigation, **Phillip Michael Parmley** is using at least one form of social media to trade child pornographic videos and images which may contain this information.

35. Based on my training and experience and my conversations with other investigations, child pornography collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes, at their private residence, for many years. The nature of the materials, their attraction to the materials, and the risk involved with receiving, downloading, and possessing such materials, motivates collectors to keep their child pornography collection within their possession and control wherever they go. Because collectors of child pornography place an extremely high value on their collection, they will take their collection with them if they move from one location to another or else keep it in a secure location nearby.

36. Collectors of child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Based on all of the above

and my training and experience, your affiant believes that **Phillip Michael Parmley** is a collector of child pornography and that child pornography is likely to be found on one or more of his electronic devices.

II. BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

37. In my training and experience, I know that cellular phones (“smart phones”), contain software and hardware that are the same, if not more sophisticated, than a typical home computer. The term “computer,” “hard drive,” and “computer media,” as used in this affidavit, also refers to cellular “smart” phones.

38. I also know that “smartphones” often allow for cloud-based storage, and many users back up their phones on their home computers. Information contained in a phone that is connected to a desktop or laptop computer, can easily transfer onto other media.

39. A computer’s ability to store images in digital form makes a computer an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

40. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

41. Collectors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, iCloud, and Hotmail, and social media applications such as Telegram, Kik and Snapchat among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online

storage of child pornography is often found on the user's computer, even if the user is accessing the information on their cellular "smart phone." Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

42. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

III. SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

43. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data

to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally difficult to accomplish this kind of data search on site; and

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

44. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

45. In addition, there is probable cause to believe that the computer and its storage devices are all instrumentalities of the TARGET OFFENSES, and thus should all be seized as such.

46. Affiant knows from training and experience that even if the files were deleted by a user, they still may be recoverable by a trained computer forensic examiner. Specifically, when a

user deletes a file, it goes into a “trash” folder. When the user directs the computer to “empty” the trash folder the contents of the folder, including the deleted file, disappear. However, the file has not left the computer and under normal circumstances, is recoverable by computer experts until it’s overwritten because there is no longer unused space in the computer’s hard drive. How soon a file will be overwritten depends on a number of factors: whether the user is computer savvy and has installed a program that accelerates the normal overwriting of deleted data, how often new files are saved to his hard drive, the capacity of the hard drive, and how the computer’s file system allocates new files. Trained certified computer forensic examiners routinely extract incriminating deleted files from hard drives, usually without difficulty.

47. Since a deleted file is not overwritten all at once, it may be possible to reconstruct it from the bits of data composing it (called “slack data”), which are still retrievable because they have not yet been overwritten even if overwriting has begun. Before a file is deleted, the file system marks it as unavailable to be overwritten. Once it is deleted, its data are no longer protected against being overwritten, but the file system won’t necessarily overwrite it all at once, and if it’s only partially overwritten computer experts can recover the portion of the data that has not been overwritten, or at least can match it to images they obtained from, for example, a website, to verify that the images were once in the computer’s hard drive and thus had been possessed. Although a savvy computer user can direct his computer to ensure quick (even instantaneous) overwriting, the default settings on standard operating systems do not do this.

48. It is difficult to know, prior to the search, which exact method of extracting the evidence will be needed and used and which specific expert possesses sufficient specialized skills to best obtain the evidence and subsequently analyze it. No matter which method is used, the data analysis protocols that will be utilized are exacting scientific procedures, designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or

encrypted files. Upon approval and execution of the search warrant, in appropriate circumstances, a forensic image (also known as a bit-stream image), which is an exact physical copy of the seized electronic evidence, will be created so that their contents could be examined at a field office or computer laboratory and/or other locations following completion of the on-site search.

49. The search of computers, hard drives, and other seized electronic media will include a complete search of the entire piece of seized electronic evidence. A computer forensic examiner cannot rely on the name of a file to exclude or confirm the existence of child pornography within that file. Individuals will intentionally mislabel directory structures, folder names, and filenames to hide the presence of child pornography. In other cases, an individual may not attempt to hide the child pornography but utilize a unique naming convention or organizational methodology which may inadvertently hide the presence of child pornography. In order to perform a comprehensive forensic examination, a computer forensic examiner must conduct an all-inclusive examination of every bit (or binary digit) on the particular electronic storage device.

50. Moreover, hard drives and other pieces of electronic media have unallocated space which might contain deleted files, records, relevant e-mails, other communications, and search terms related to the possession, receipt, and distribution of child pornography. Thus, without looking at the entirety of the electronic media for evidence related to child pornography, the investigator may not find evidence relevant to the criminal investigation.

IV. SEARCH METHODOLOGY TO BE EMPLOYED

51. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. on-site triage of computer system(s) to determine what, if any, peripheral devices and/or digital storage units have been connected to such computer system(s), as well as a

preliminary scan of image files contained on such system(s) and digital storage device(s) to help identify any other relevant evidence and/or potential victim(s);

b. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

c. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

d. surveying various file directories and the individual files they contain;

e. opening files in order to determine their contents;

f. scanning storage areas;

g. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or

h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

USE OF BIOMETRIC FEATURES TO UNLOCK ELECTRONIC DEVICES

52. The warrant I am applying for would permit law enforcement to compel **Phillip Michael Parmley** to unlock a device subject to seizure pursuant to this warrant that is his possession or for which law enforcement otherwise has a reasonable basis to believe is used by him using the device's biometric features. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. I have probable cause to believe that one or more of the electronic devices in the SUBJECT PREMISES are likely to offer its user the ability to use biometric features to unlock the device(s). Telegram is a social media application that can be accessed by a cellular telephone. Your affiant knows that many smart phones use fingerprint sensor technology and facial recognition to unlock the phone and believes that **Phillip Michael Parmley** is likely to have a smart phone, utilizing telephone number (636) 385-3509.

c. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

d. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called “Trusted Face.” During the Trusted Face registration process, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes

and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

e. If a device is equipped with an iris recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

f. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

g. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

h. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

53. Due to the foregoing, if law enforcement personnel encounter a device that is subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, and the device is in **Phillip Michael Parmley**'s possession or law enforcement otherwise has a reasonable basis to believe is used by **Phillip Michael Parmley**, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of **Phillip Michael Parmley** to the fingerprint scanner of the device(s) found at the premises; (2) hold the device(s) found at the premises in front of the face of **Phillip Michael Parmley** and activate the facial recognition feature; and/or (3) hold the device(s) found at the premises in front of the face of **Phillip Michael Parmley** and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

CONCLUSION

54. Based on the foregoing I submit that this affidavit supports probable cause for a warrant to search the Premises described in Attachment A and seize the items described in Attachment B.

I state under the penalty of perjury that the foregoing is true and correct.



David Rapp
Special Agent
Federal Bureau of Investigation
(314) 341-7246 (Cell)

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 on April 10, 2020.

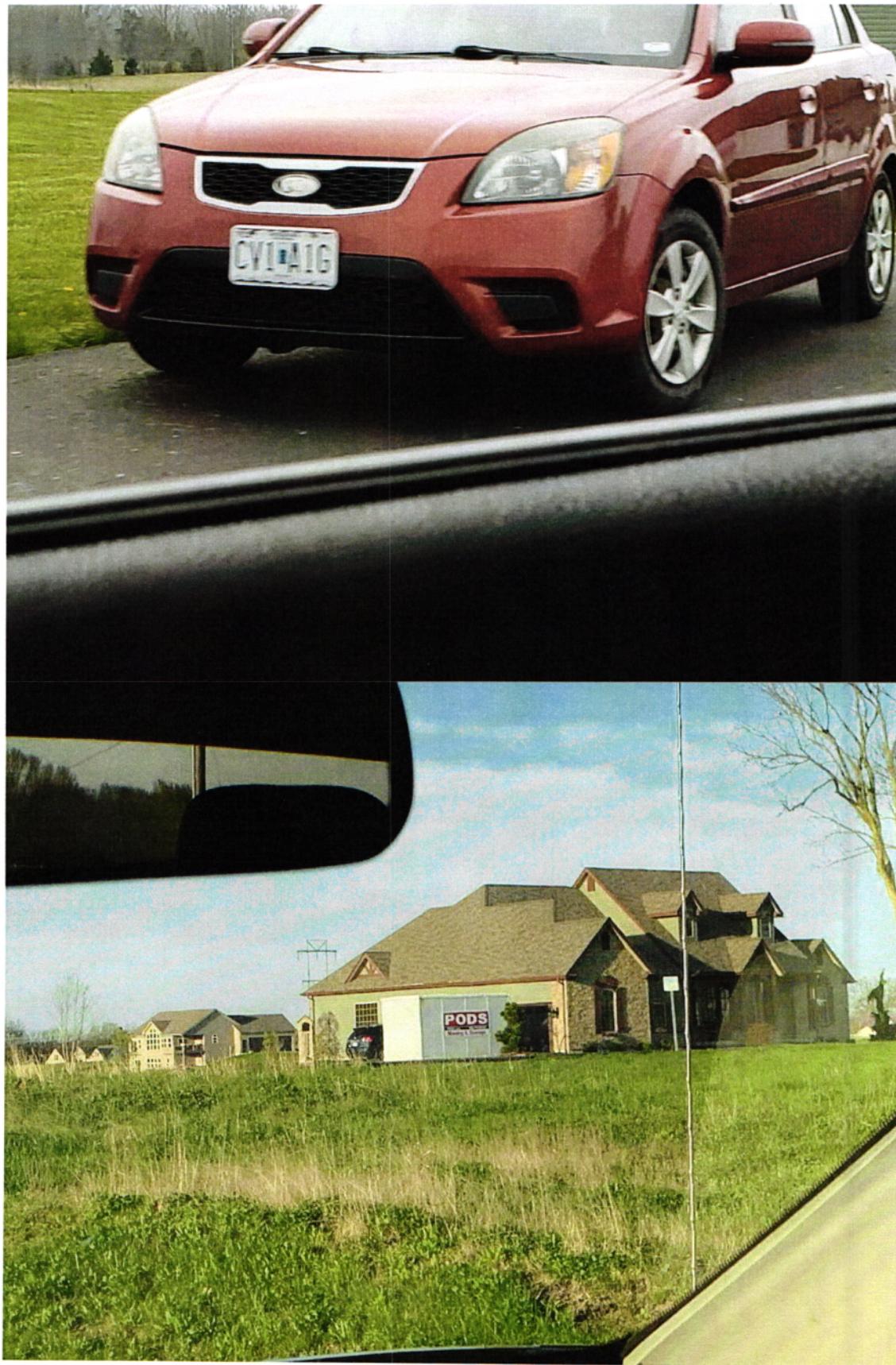
/s/ David D. Noce

Honorable David D. Noce
United States Magistrate Judge

ATTACHMENT A
DESCRIPTION OF LOCATION TO BE SEARCHED

The location to be searched (here "SUBJECT PREMSIES") is: 11830 Claremont, Wright City, MO, 63390, and is identified as follows: The residence is a single family home, with a detached garage, that is brown in color with tan brick, and is a 3 bedroom, 2.5 bath, approximate 2,500 square foot in size and on an approximate 3 acre lot. The residence is listed on Accurint as being owned by Ronald Parmley and Sandra Boyd. The SUBJECT PREMISES includes, but is not limited to: a large, approximate 16 feet in length PODS container located on the driveway, and any vehicles located on the premises and under the control of **Phillip Michael Parmley**, to include, a 2010 Kia Rio, Missouri License Plate CV1A1G.





ATTACHMENT B
LIST OF ITEMS TO BE SEIZED

The following are to be seized from the SUBJECT PREMISES: evidence, instrumentalities and contraband concerning the violations of 18 U.S.C. §§ 2252A(a)(2) (Receipt of Child Pornography) and 2252A(a)(5)(B) (Possession of Child Pornography) (hereafter referred to as the “TARGET OFFENSES”) as follows:

1. All visual depictions, including still images, videos, films or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, and any mechanism used for the distribution, receipt or storage of the same, including but not limited to:
 - a. Any computer, cell phone, computer system and related peripherals including and data processing devices and software (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, routers, PDA's, gaming consoles, cell phones, computer compact disks, CD-ROMS, DVD, and other memory storage devices) (hereinafter referred to collectively as Devices);
 - b. peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, scanners, digital cameras, and related communications devices such as cables and connections); and
 - c. any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

2. Any and all computer passwords and other data security devices designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.
3. Any and all documents, records, emails, and internet history (in documentary or electronic form) pertaining to the possession or production of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or pertaining to an interest in child pornography whether transmitted or received.
4. Any and all records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use of computer equipment found in the residence.
5. Documents and records regarding the ownership and/or possession of the SUBJECT PREMISES.
6. During the course of the search, photographs of the SUBJECT PREMISES may also be taken to record the condition thereof and/or the location of items therein.
7. During the execution of the search of the Premises described in Attachment A, law enforcement personnel are also specifically authorized to obtain from **Phillip Michael Parmley** at the time of execution of the warrant, the display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock any Devices requiring such biometric access subject to seizure pursuant to this warrant, that is, including pressing fingers or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition, of:
 - (a) any of the Device(s) found at the SUBJECT PREMISES,

(b) where the Device(s) are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments, for the purpose of attempting to unlock the Device(s)'s security features in order to search the contents as authorized by this warrant.